

substantial benefits for individuals, businesses, and society as a whole. Because these benefits can be produced with minimal costs to business, NTIA expects that the private sector will have strong incentives to voluntarily implement the modified contractual framework outlined below. If such private sector action is not forthcoming, however, that framework can and should form the basis for government-mandated privacy regulations or standards.

A. Notice

The notice component of NTIA's modified contractual framework is grounded in the principles of fair information practices released by the IITF's Privacy Working Group in June 1995, after two years of deliberation, including field hearings and two rounds of public comment.⁸³ At the crux of these principles is the Notice Principle, which states:

Information users who collect personal information directly from the individual should provide adequate, relevant information about:

1. *Why they are collecting the information;*
2. *What the information is expected to be used for; [and]*
3. *What steps will be taken to protect its confidentiality, integrity, and quality*⁸⁴

Adequate notice requires that consumers be informed about how personal information is collected, processed, exchanged, disclosed, and used in our rapidly evolving information infrastructure.⁸⁵ In any particular transaction, an individual should have adequate information on which to decide whether to accept the offered service under the clear terms concerning the use of personal information. Such notice should be conspicuous and in plain language so that consumers have the necessary information to exercise sound judgment about the level of privacy

83 *IITF Principles*, *supra* note 11. Those principles begin with the Information Privacy Principle, which states: "Personal information should be acquired, disclosed, and used only in ways that respect an individual's privacy." *Id.* at Commentary sec. I.A. The remaining principles create a framework that places rights and responsibilities on individuals and information users so that the Information Privacy Principle is satisfied.

84 *IITF Principles*, *supra* note 11, at Commentary sec. II.B. *See also* Organization for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Purpose Specification Principle at 10 (Paris 1981) [hereinafter *OECD Guidelines* ("The purposes for which personal data are collected should be specified not later than at the time of data collection . . .")].

85 An important corollary to the Notice Principle is the Fairness Principle, which insists that information users keep their promise to the individual by abiding by the terms set out explicitly in their notice, or, in the absence of notice, by respecting the individual's reasonable contemplation of how personal information will be used. *See IITF Principles*, *supra* note 11, at Commentary sec. II.D. *See also OECD Guidelines*, *supra* note 84, Use Limitation Principle at 10 (stating that "Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except with the consent of the data subject or by the authority of law."). Indeed, the Notice Principle would amount to mere formalism if information could be used in ways completely divergent from the individual's understanding.

protection that they desire and what is available to them.⁸⁶ It must clearly instruct the consumer that a choice is required, and it must reach the consumer *before* the company uses the TRPI for unrelated purposes.

These criteria provide a framework against which “adequacy” may be assessed. When personal information is collected and used only to render a service, explicit notice may not be required because the individual is already aware of the extent of that information’s collection and use. For example, if a company sells long distance service to an individual, that company ought to be able to use TRPI to detail the customer’s calling patterns and to develop a long distance offering that better suits the consumer’s needs. However, for uses unrelated to the original service offering, consumers may have no such expectation and, indeed, may have given little thought to how their TRPI could be used. Put another way, a consumer’s decision to purchase one service cannot reasonably be seen as tacit consent for company use of TRPI to develop and market another service. Thus, telecommunications and information service providers should give their customers plain and conspicuous notice of any unrelated or ancillary use of their TRPI.⁸⁷

Notice requirements should also change as telecommunications and information companies become multiple service providers. For instance, local exchange carriers will likely offer a variety of different services, including access to the Internet and interactive multimedia services in addition to local telephone service. Although many consumers might have implicitly understood, in the past, that phone companies would use information collected about them for offerings tailored to their particular needs, subscribers to these more advanced networks may not understand that TRPI collected about them for telephone and video service purposes could also be used to sell them on-line shopping services, for example. As a result, more explicit notification may be needed for subscribers of multiple service networks to understand how their TRPI will be used for internal customer marketing purposes.⁸⁸

There may be a range of notice procedures that will adequately inform consumers about the intended use of their TRPI, while minimizing costs for industry and, ultimately, customers. For some service providers, notice can most easily be given at their first contact with prospective

86 In a limited number of circumstances, merely notifying a customer of a company’s policies and practices with respect to TRPI will not be enough. For example, when a prospective customer’s primary language is not English, it is incumbent on the service provider to take steps to ensure that notice is not merely given but understood.

87 Similarly, provisions under the pending House telecommunications reform legislation, H.R. 1555, would prohibit carriers from disclosing or using CPNI for purposes other than to provide a particular service, without subscriber permission.

88 Recognizing that privacy is a “core value in modern society,” Microsoft developed a set of principles for how customer information is gathered, processed, used and stored over its on-line Microsoft Network (MSN). These principles include provisions for notifying subscribers about how information about them will be collected and used and imposes limitations on how information can be used by MSN content providers. For example, a content provider may be asked “to specify the legitimate business purpose for gathering information from a Member and to provide that Member with the opportunity to opt-out of the processing or use of that information for direct marketing purposes.” MSN, *The Microsoft Network, Summary of Principles on Gathering, Processing, Using and Storing Member Information* (July 1, 1995).

customers. For example, when individuals subscribe to most on-line information services, such as CompuServe or Prodigy, they are typically given several choices concerning dissemination of their TRPI, including the option not to have such information disclosed at all. Other companies may find it more cost effective to include a privacy notification in the written materials they send to consumers to confirm the terms and conditions of their service agreement. Still other firms may provide notice as one of the myriad inserts that they commonly include in their customers monthly bills. If the notification meets the criteria outlined above, it should adequately address the needs of consumers.⁸⁹

This approach gives companies sufficient flexibility that they should be able to notify their customers about their information practices without incurring excessive costs. When firms receive service requests from customers over the phone, companies typically spend time to collect a wide range of information from those customers. Similarly, companies commonly send a mass of written materials to their current and prospective customers, seeking to interest them in new services. The incremental costs of including a privacy notification in those phone conversations or those written solicitations should not be significant.

B. Consent

The other fundamental component of NTIA's privacy framework is customer consent. Notifying consumers of company practices concerning TRPI would have little practical effect if consumers did not have a meaningful opportunity to accept or reject the terms offered. Indeed, in those service markets dominated by a single supplier—such as local telephone service and the delivery of multichannel video programming to the home, the absence of any consent requirement would give consumers only a Hobson's choice—between accepting company TRPI policies that do not provide an acceptable level of privacy protection and foregoing a highly desired, even essential service.

Most companies agree that individuals should have the right to limit or prohibit ancillary or unrelated uses of personal information, such as disclosing information to third party marketers. In the words of the Direct Marketing Association (DMA)⁹⁰—whose membership includes many communications providers:

Consumers who provide data that may be rented, sold, or exchanged for direct marketing purposes periodically should be informed of the potential for the rental, sale,

89 A company should generally not be required to provide its customers with recurrent notices about its privacy policies. Such requirements would merely impose costs on businesses—most of which may be passed on to consumers. Thus, after the first notice has been given, a company should provide additional notices only if there has been a change in its privacy policies and practices.

90 DMA has produced industry guidelines for "Ethical Business Practices," "Personal Information Protection," "Telephone Marketing," "Acceptance of Print Advertising," "Mailing List Practices," "Broadcast Advertising," and a "Fair Information Practices Checklist." Comments of DMA at 5-6.

*or exchange of such data. Marketers should offer an opportunity to have a consumer's name deleted or suppressed upon request.*⁹¹

*Consumers who provide data that may be rented, sold, or exchanged for marketing purposes should be informed . . . of the opportunity to opt-out of the marketing process.*⁹²

Similarly, Time Warner encourages the use of the Department of Health, Education and Welfare's 1973 privacy principles which, among other things, state that "[i]ndividuals should have the ability to limit the disclosure of information about them that was obtained for one purpose from being disclosed for other unrelated purposes."⁹³

The more controversial policy issue is how consumer consent should be obtained. That debate centers around two contending concepts—"opt-in" and "opt-out."⁹⁴ Under an opt-in approach, companies cannot use TRPI for ancillary purposes until the individual first gives consent. In an opt-out program, information can be used in an ancillary manner unless the individual affirmatively opts-out of such practices within some allotted time. Opt-in thus requires expressed consent: an individual's silence means that the information *cannot* be used. Opt-out garners tacit consent: silence means that the information *can* be used.

The choice between opt-in and opt-out is not a simple one. Although privacy is a fundamental personal right that must be adequately protected, it is also true that the level of privacy protection desired varies widely among consumers. Furthermore, the free flow of

91 DMA Guidelines for Personal Information Protection, Art. 5 in Direct Marketing Association, Inc., *Fair Information Practices Manual: A Direct Marketer's Guide to Effective Self-Regulatory Action in the Use of Information* (Oct. 1994) [hereinafter *Fair Information Practices Manual*]. This document provides direct marketers with information about how to implement corporate fair information policies and how to comply to these self-regulatory programs. DMA has received approximately 1,000 requests from industry for this manual since its release.

92 DMA Guidelines for Ethical Business Practice, Art. 32 in *Fair Information Practices Manual*.

93 Comments of Time Warner Inc. at 6. The five basic principles of this code are: 1) Personal data record-keeping practices should not be kept secret; 2) Individuals should have the ability to find out what information about them is on record and how it is disclosed; 3) Individuals should be able to correct or amend records of identifiable information about them; 4) Individuals should be able to limit the disclosure of information about them that was obtained for one purpose from being disclosed for other unrelated purposes; and 5) An organization creating, maintaining, using, or disseminating records of identifiable personal data must guarantee the reliability of the data for their intended use and must take precautions to prevent misuse of the data. *Id.* at 4-5; see also *DHEW Principles*, *supra* note 11.

94 Congress grappled with this very issue with respect to telemarketing sales calls before passing the Telephone Consumer Protection Act of 1991, which, among other things, requires telemarketers to consult a list of persons who do not wish to receive telephone sales calls and prohibits telemarketers from calling them. See 47 U.S.C. §227. In the end, Congress chose to balance the concerns of an emerging industry and consumers by deciding in favor of an opt-out approach and establishing a national clearinghouse that would maintain a list of consumers who did not wish to be called. *Id.*

information—even personal information—promotes a dynamic economic marketplace, which produces substantial benefits for individual consumers and society as a whole.

Not surprisingly, many service providers argue that securing customer consent through an opt-in procedure “could harm innovation and prevent desirable services from emerging.”⁹⁵ They also contend that individuals cannot accurately predict today what they may find useful tomorrow. As a result, an opt-in approach may prevent uses of personal information that individuals may in fact want.⁹⁶ In fact, in a national survey conducted by Louis Harris, a majority of consumers polled (52%) indicated that they would be interested in participating in subscriber profiling activities—receiving advertising and information about products and services matching their particular interests—over interactive networks, and 48 percent would be “somewhat” interested in supplying information that would enable them to receive special offers.⁹⁷ On the other hand, it may be argued that individuals cannot accurately predict how seemingly innocuous information may be used in inappropriate ways. Thus, an opt-out approach may lead to uses of personal information that individuals would reject.

NTIA believes, on balance, that the mechanism for securing customer consent for company use of TRPI should depend on the nature of that information. Companies should not make any ancillary use of “sensitive” TRPI without first obtaining explicit authorization from the relevant customer. On the other hand, a company should be allowed to use non-sensitive TRPI for unrelated purposes unless the customer affected, having been notified of the company’s plans, takes some action stopping such use—such as making a telephone call or mailing in a form—by a certain date.⁹⁸ When the date for customer action has passed—but not before—the company should be free to use the customer’s TRPI in the ways identified. Whatever the mechanism for securing customer consent, however, consent should never be a precondition for receiving service. That is to say, subscribers may not be denied service because they decline to authorize use of their TRPI for purposes other than rendering the service requested.⁹⁹

95 Comments of Bell Atlantic at 4. *Cf.* Comments of AT&T at 9-10; Comments of Time Warner Inc. at 12; and Comments of The Newspaper Association of America at 2, 3-4 (all favoring an opt-out approach).

96 See Comments of TRW Inc. at 11-12.

97 Louis Harris and Associates, Inc., *Interactive Services, Consumers, and Privacy: A National Survey* 94 (1994). However, this same group expressed privacy concerns. For example, 60% indicated that they would like to be fully informed about a provider’s collection of subscriber profile information before deciding to subscribe to its services; 74% indicated that they would like to review the information in their profile, correct errors, and indicate which sets of information they would allow to be used for marketing. *Id.* at 95.

98 The distinction between sensitive and non-sensitive data is not clear-cut; information that is sensitive to one person may be innocuous to another. Although NTIA does not suggest a definitive answer to this question, we do believe that information relating to health care (*e.g.*, medical diagnoses and treatments), political persuasion, sexual matters and orientation, and personal finances (*e.g.*, credit card numbers) should be considered “sensitive.” The same is true for an individual’s social security number, which has become a universal personal identifier, a passkey that allows the holder to unlock and accumulate the vast storehouse of information on most people that is available from a host of different databases.

99 See generally Comments of The Consumer Interest Research Institute at 8.

Requiring affirmative consumer consent in the case of sensitive information is consistent with the intuition that individuals should have greater control of sensitive information because of the greater harm that improper disclosure or use of such information may cause.¹⁰⁰ It has the added benefit of minimizing the aggregate transaction costs in obtaining an individual's authorization. Many individuals would likely reject the ancillary use of sensitive TRPI. Instead of requiring the many who reject the ancillary use from bearing the transaction costs of opting-out, it is more efficient to require the few who approve that use to opt-in. On the other hand, because most people would likely not object to ancillary use of non-sensitive TRPI, it makes sense to give the responsibility of protecting that information to the few consumers who want it protected.

The promised interactivity of the NII may diminish the need to make a policy choice between opt-in and opt-out. Such interactivity would make it possible for service providers to obtain consent to use TRPI from subscribers electronically before any services were rendered. This development would reduce the need for privacy protection policies that impede the flow of information exchange by creating "a process that requires mailing out consent forms, waiting for them to return, and then processing them before any data can be used or collected."¹⁰¹ It would also allow providers greater flexibility to construct a variety of contract levels with subscribers for use of their TRPI, while leaving it up to consumers to ultimately determine which levels of access and use of their TRPI they will allow.

NTIA also recognizes the importance of enhanced consumer education in this area.¹⁰² Education serves two purposes: empowerment—giving consumers control of how their personal information is used; and understanding—helping consumers to understand how their personal information can be used in beneficial ways, thereby increasing their willingness to use the NII. Similar to the efforts of some Bell companies to educate consumers about their options for handling unwanted sales calls according to the provisions of the TCPA,¹⁰³ NTIA recommends

100 The IITF Fairness Principle states that "the nature of the incompatible use will determine whether such consent should be explicit or implicit. In some cases, the consequences to an individual may be so significant that the prospective data user should proceed only after the individual has specifically opted into the use by explicitly agreeing." See *IITF Principles*, *supra* note 11, at Commentary ¶ 22.

101 See Comments of Time Warner at 12.

102 The IITF's Education Principle also recognizes the importance of enhanced consumer education. See *IITF Principles*, *supra* note 11, at Commentary sec. II.E.

103 A report conducted by the staff of the House Subcommittee on Telecommunications and Finance found that Bell Atlantic-Maryland had undertaken efforts to educate its customers about how to avoid unwanted intrusions from telemarketers through billing statements. See Letter from Edward J. Markey, Chairman, Subcommittee on Telecommunications and Finance, U.S. House of Representatives, to Mr. Sam Ginn, Chairman and CEO of Pacific Telesis Group (July 14, 1994) (on file at NTIA).

Pacific Telesis Group has also taken a number of steps to educate its consumers about avoiding unwanted telemarketing sales calls. For instance, Pacific Telesis Group's subsidiaries—Pacific Bell and Nevada Bell—include a "Consumer Rights and Information" section in their directories and bill inserts which describe how consumers can handle telephone sales calls. A 24-Hour Customer Guide Information Line also offers audiotext messages about how to use the phone, including information on how to "reduce sales calls." See Letter from

that industry work with consumer advocacy organizations, industry associations, and community groups to more effectively educate consumers about their opportunities to limit disclosure of TRPI.¹⁰⁴ Consumer education should be an integral part of any effective provider notification policy.

IV. CONCLUSION

Although the United States currently has a number of laws and regulations governing private sector acquisition, use, and disclosure of TRPI, those provisions are limited in scope and inconsistent in application. They generally are confined to a specified group of existing services, and do not apply to all providers of any one service. Developed to address particular problems in particular circumstances, prevailing privacy protections in this area do not apply to many of the next generation of services that are rapidly arriving and could not readily be adapted for that purpose.

Some remedial action is warranted. The privacy framework described in this paper enables service providers and their customers to come to mutually agreed upon contracts regarding the use of TRPI independent of government intervention. The advantages for consumers and the private sector are obvious. Consumers benefit from a privacy standard that affords them with the same TRPI safeguards for like services across the communications sector. Uniform, effective and understandable privacy protections should also reduce a major potential barrier to consumer use of the NII as consumers better understand how their personal information is used and exercise their right to control its use. Increased public confidence in how personal information is acquired, disclosed, and used could thereby stimulate consumer demand for the many services that businesses will seek to offer over that network of networks.

Uniform privacy requirements will further benefit the private sector by eliminating a potential source of competitive advantage or disadvantage among rival providers of telecommunications and information services. At the same time, NTIA's recommended approach gives private firms considerable flexibility to discharge their privacy obligations in a way that minimizes costs to the firms and to society. For all of these reasons, NTIA believes that both consumers and the private sector will benefit substantially from voluntary implementation of that approach. If, however, industry self-regulation does not produce adequate notice and customer consent procedures, government action will be needed to safeguard the legitimate privacy interests of American consumers.

P.J. Quigley, Chairman, President and Chief Executive Officer, Pacific Telesis Group, to Hon. Edward J. Markey, Chairman, Subcommittee on Telecommunications and Finance, U.S. House of Representatives (June 26, 1995) (on file at NTIA).

104 The Privacy Rights Clearinghouse recommends in its comments that consumer education, among other things, should include "plain language descriptions of how new technologies affect privacy, explanations of consumers' legal privacy rights, [and] guidelines for effective consumer-privacy practices." See Comments of the Privacy Rights Clearinghouse at 3.

Ultimately, defining the balance between the free flow of information and an individual's right to privacy over an NII revolves around trust. If consumers feel that their personal information will be misused or used in ways that differ from their original understanding, the commercial viability of the NII could be jeopardized as consumers hesitate to use advanced communications networks. Whether through government intervention or industry self-regulation, consumers will have to feel comfortable with how personal information is used, and with their ability to control its use in a meaningful way.

APPENDIX A: MARKETING PROFILES

So, we can look at your customers and tell you a lot more about them. More than you ever thought possible. And not as a group, but as individuals. By exact age. Sex. Income. Lifestyle characteristics. Life event. And more. And we can help you decide the most effective ways to use this type of information to achieve your marketing goals.

Advertisement of Metromail, Inc.¹

In addition to communications providers, many other parties will also have access to consumer information on the NII. These others include transacting parties, such as merchandisers, that do business with individuals via telecommunications but have no role in the communications service itself. They also include other types of transaction facilitators, such as electronic payment providers, that help individuals and transacting parties execute their transactions.

The enormous variety of transacting parties and transaction facilitators makes it impossible to analyze the particular privacy concerns associated with each party. One common thread, however, links how nearly all these players seek to use TRPI: to create marketing profiles. A marketing profile is a record of an individual's characteristics created by acquiring personal information from multiple sources and used to target products and services. Given the impossibility of analyzing each type of transacting party and transaction facilitator, it makes sense to explore the privacy issues implicated by this one common thread.²

The general subject of marketing profiles does not fall squarely within the scope of this paper because, as explained below, such profiles comprise information not classified as TRPI. Nevertheless, an examination of marketing profiles is germane to this paper for two reasons. First, the electronic nature of TRPI makes it inexpensive to access and combine into marketing profiles. Second, as more daily transactions take place on the NII, more TRPI will be available to be incorporated into profiles.³

1 Metromail, *The New Marketing: Selling in the Age of the Individual* 7 (1994) (brochure).

2 The privacy issues associated with communications providers, which have already been discussed, are not revisited here. Profiles used to determine whether an individual receives consumer credit is governed by the Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1618a - 1681t (1988). Such profiles are also outside the scope of this appendix.

3 Not all personal profiles are compiled for marketing purposes. Certain profiles are created, for example, to aid private investigators, media, and lawyers in search of missing individuals and their assets. See Teresa Pritchard-Schoch & Susan Hutchens, *Remote Access to Public Records: An Update*, Database, Feb. 1994, at 14.

I. BACKGROUND

A. Marketing Profiles: The Heart of Targeted Marketing

Selling personal information is big business. By one estimate, it has risen to a \$3 billion per year industry and generates more than ten thousand different types of lists,⁴ brokered by more than one thousand commercial services.⁵ At the heart of this information industry is the marketing profile. Marketing profiles are created and used by the private sector to maintain old customers and to target new ones. Companies sift through their internal records of customer purchases—who bought what, when, how often, and for how much—in order to identify and cater to their most profitable customers.⁶ For example, certain merchandisers now have computerized marketing profiles in “client books,” which give salespeople immediate access to “the preferences and sizes of frequent customers.”⁷ Using statistical modeling techniques, companies also use their sales records to determine the attributes of the “model customer” most likely to purchase a particular product or service.⁸ Actual marketing profiles are then compared with this model profile to identify those persons warranting solicitation.⁹

To refine this solicitation process, companies enrich their proprietary databases with information available from major list-compilers, which maintain sizeable national consumer databases on American households.¹⁰ A list-compiler will enrich and analyze the company’s proprietary personal information, develop a profile of the model customer, and identify

4 See Jill Smolowe, *Read This!!!!!!!*, Time, Nov. 26, 1990, at 62, 66 (referring to the *Direct Mail List Rates and Data* published by the Standard Rate & Data Service). An average person appears on one hundred mailing lists and fifty databases. See Anne Wells Branscomb, *Who Owns Information?: From Privacy to Public Access* 11 (1994).

5 See Charles Piller, *Privacy in Peril*, MacWorld, July 1993, at 8, 11 (describing contents of the Burwell Directory of Information Brokers).

6 See Laura Bird, *Department Stores Target Top Customers*, Wall St. J., Mar. 8, 1995, at B1 (“Such department stores as Bloomingdale’s, Nordstrom and Saks Fifth Avenue are starting to tap their vast customer databases to identify their most profitable shoppers.”).

7 *Id.*

8 See David Zielinski, *Database: the Heart of Relationship Marketing*, 27 Potentials in Marketing 66 (1994); Jonathan P. Graham, Note, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 Tex. L. Rev. 1395, 1401 (1987) (discussing how computers are used to produce “psychographics”—psychological profiles of consumers) (emphasis added).

9 See generally Jonathan Berry, *Database Marketing*, Bus. Wk., Sept. 5, 1994, at 56-61.

10 For example, the consumer information database of Donnelley Marketing Inc. contains “consumer data on over 150 million individuals and 90 million households.” Donnelley Marketing Inc., *Donnelley Marketing Inc. Consumer Information 1* (brochure). Metromail advertises a database of 133 million people. See Metromail, *supra* note 1.

“profile clones” from its national database as prospective customers.¹¹ Or, if a company knows exactly what type of person to solicit, the list-compiler can provide a customized list of names, addresses, and telephone numbers by geographical site. For example, list brokers have created catalogs of “Arabs, in Their Native Lands, Who Gamble and Invest;” “Doctors Who Are Known to Have Gambled;” and “Jewish Philanthropists and Investors.”¹²

B. Sources of Information for Marketing Profiles

The personal information found in marketing profiles comes from three sources: public records; internal records—records collected directly from the individual by the profiler; and external records—records obtained by the profiler not directly from the individual but from some third party.

Public records are records collected by the government pursuant to various research, licensing, administrative, and adjudicatory schemes, that are somehow made available for public inspection. Depending on the state, such records could include “census tract data, county assessments, deed transfer records, electoral records, suits, liens, and judgments, [and] business and professional licensing records.”¹³ They may also include automobile registration, driver’s license registration, birth records, and death records. Finally, they even include the National Change of Address (“NCOA”) file, sold by the United States Post Office to those tracking individuals on the move.¹⁴ Public records can reveal volumes about an individual. Moreover, based on this information, profilers can make educated guesses about other characteristics, such as income.¹⁵

Internal records are records collected by the profiler directly from the individual. As previously noted, both transacting parties (*e.g.*, clothier) and transaction facilitators (*e.g.*, credit card company) can collect various forms of TRPI in the course of an NII transaction. Given the marketing value of such information, many profilers analyzing their customers and subscribers are “aiming for 100% information capture” in the course of any single transaction.¹⁶

11 “Companies can now buy lists of customers who have bought products similar to their own, or who share characteristics, and merge them with other databases giving further information on the individuals named.” Alan Shipman, *Scanned and Deliver: Mailshot Marketing*, 49 Int’l Mgmt. 27 (1994).

12 See Bill Granger, *The Name Traders*, Chi. Trib., Nov. 15, 1992, (Magazine), at C22.

13 Comments of Mead Data Central, Inc. and Dun & Bradstreet Corp. at 3.

14 Until recently, the Post Office released Change of Address information for a particular person to anyone for a \$3 fee. In 1994, the Post Office discontinued that practice. However, the Post Office continues to sell the entire NCOA (principally to mass mailers). Representative Gary Condit has introduced the “Postal Privacy Act of 1995,” H.R. 434, 104th Cong., 1st Sess. (1995), which would require notice and opt-out for NCOA forms.

15 Income is often estimated on the basis of census neighborhood information, real property records, and vehicle registration.

16 See Bird, *supra* note 6, at B1.

Finally, *external records* are records obtained by the profiler not directly from the individual but from some third party. These third parties include, for example, social and political organizations; news and entertainment publications; and merchandisers that sell their internal records about members, subscribers, and customers to outside profilers. Profilers can obtain external records at different levels of detail. Consider, for instance, the external records that a profiler could obtain from a general clothier in a virtual mall. The profiler could rent a *complete mailing list* of the clothier's entire clientele. Such a list could include only the name and address (e-mail or postal) of every customer who ever made a purchase. The profiler could also buy a customized mailing list of some subset of the clothier's clientele, such as the names and addresses of customers who have purchased lingerie from the clothier in the last two years. Finally, the profiler could obtain more than just names and addresses and obtain *transactional data*, detailing additional fields of information in the clothier's internal records. This could include, for example, product purchased (*e.g.* large, red, cotton sweater), time and date, and purchase price.

By drawing from all three sources of information—public records, internal records, and external records—profilers may have a detailed marketing dossier, which includes demographic and psychographic information. A profile available from a national-list compiler could include: name, gender, address, telephone number, age, estimated income, household size and composition, dwelling type, length of residence, car ownership, pet ownership, responsiveness to mail offers, contributor status, credit card ownership, lifestyle, hobbies, interests, and neighborhood characteristics including average education, house value, and racial composition. This information could be added to whatever additional TRPI—revealing specific communications, purchases, services, and other transactions—in a profiler's possession.

II. THE PRIVACY ENVIRONMENT

A. Legal Environment

The creation of marketing profiles involves first, accessing personal information, and second, matching it to a particular individual. Theoretically, legal constraints on the creation of marketing profiles could exist at each stage of the profile development process.

1. Access

As discussed in the main body of this paper, a patchwork of Federal and state laws regulate the private sector's access to certain types of personal information. Of the three categories of information mined by profilers—public records, internal records, external records—access to *public records* is least restricted. This is because by definition, public records are made available to the public in some form, to serve some public interest such as maintaining open and accountable government. Nevertheless, access and use of certain public records have been somewhat limited despite their "public" nature. For example, various states, such as California, forbid voter registration rolls from being used for commercial

purposes.¹⁷ Another important example is the recently enacted federal Driver's Privacy Protection Act of 1994.¹⁸

Internal records are records collected by the profiler directly from the individual in the course of some transaction. The law can restrict a profiler's access to internal records in two ways. First, it can limit collection of TRPI to the degree that is functionally necessary. Second, the law can require the profiler to purge its internal records after it becomes no longer functionally necessary to keep.¹⁹ For example, the Cable Act contains both types of provisions. Even though a cable operator has the technological capability to collect more TRPI than is necessary to render cable service, the Act bars them from taking advantage of that capability, unless it obtains the individual's consent. Second, a cable operator must destroy personal information when no longer necessary.²⁰

The Cable Act is the exception, not the rule. The law generally does not limit a profiler's collection of TRPI in the course of transacting with an individual or facilitating that transaction. Furthermore, the law does not generally require profilers to purge their internal records after some established period. In sum, the law leaves transacting parties and transaction facilitators free to collect whatever TRPI they can and to keep whatever information they collect.

The law does put various constraints on profilers from accessing certain types of *external records*. Federal and state laws protect to varying degrees the confidentiality of certain bank, credit, medical,²¹ cable, electronic communications, and videotape rental information. But access to many other types of external records is unrestricted. Significantly, no Federal law limits a profiler's ability to access TRPI held by payment providers, such as credit card companies. Credit card companies, some of which keep permanent records of a cardholder's transactions, "can name each cardholder's favorite restaurants and vacation spots, their hobbies and where they shop for gifts."²² These companies can compile the information from an individual's credit card purchases—the merchant, the item, the amount, and the date—and sell it to profilers without federal restrictions.

17 See Rick Wartzman, *Information, Please: A Research Company Got Consumer Data from Voting Rolls*, Wall St. J., Dec. 23, 1994, at 1 (referring to Cal. Elections Code § 2194 (Deering 1994)).

18 See 18 U.S.C. §§ 2721-2725 (1988 & Supp. V 1994).

19 47 U.S.C. § 551(b), (e) (1988 & Supp. V 1993). Similarly, the Video Privacy Protection Act of 1988 requires the destruction of "personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected" 18 U.S.C. § 2710(e) (1988 & Supp. V 1994).

20 47 U.S.C. § 551(b), (e) (1988 & Supp. V 1993).

21 See, e.g., N.Y. Pub. Health Law § 17 (Consol. 1994) (records of sexually transmitted disease or abortion for a minor cannot be disclosed, even to parent).

22 John Healy, *Just Between Us*, Cong. Q., May 14, 1994, at 41.

2. Matching

Besides access, legal constraints on the creation of marketing profiles could also conceivably be placed on the matching of lawfully obtained data into a marketing profile. For example, computer matching performed by federal agencies is somewhat regulated by the Computer Matching and Privacy Protection Act of 1988 ("Matching Act").²³ In contrast to this restraint on federal government agencies, no regulations govern the way that private sector profilers may match personal information once it is properly accessed. In other words, once a profiler legally acquires personal information, the profiler is free to sort that information by individual and compile it into a marketing profile. Indeed, many commenters argued that governmental interference with how private parties "match" information legally obtained would infringe the First Amendment.²⁴

B. Market Environment

Even though the access and matching of TRPI into marketing profiles are not substantially regulated by law, the "law of the market" may nevertheless prompt adequate self-regulation. As succinctly observed by one commenter, "companies do not prosper by alienating customers."²⁵ For instance, market forces have prevented certain marketing profile products from reaching the market. Lotus Development Corporation, a software company, and Equifax, one of the nation's largest credit reporting bureaus, abandoned plans to market a CD-ROM database called "Marketplace: Households" in the face of widespread public criticism.²⁶ Many commenters pointed to such incidents as evidence that the marketplace protects privacy interests adequately and that governmental regulation is unneces-

23 5 U.S.C. § 552a(o)-(q) (1988). The Computer Matching and Privacy Protection Act of 1988 (Pub. L. No. 100-503) has amended the Privacy Act to add several new provisions. See 5 U.S.C. § 552 (a)(8)-(13), (e)(12), (o), (p), (q), (r), (u), (1988 & Supp. V 1993). These provisions add procedural requirements for agencies to follow when engaging in computer-matching activities; provide matching subjects with opportunity to receive notice and to refute adverse information before having a benefit denied or terminated; and require that agencies engaged in matching activities establish Data Protection Boards to oversee those activities.

More recently, Congress enacted the Computer Matching and Privacy Protection Amendments of 1990 (Pub. L. No. 101-508), which further clarify the due process provisions found in subsection (p). Office of Information and Privacy, U.S. Dep't of Justice, *Freedom of Information Act Guide & Privacy Act Overview* 458-59 (Sept. 1994).

24 Various commenters assert that governmental restrictions on the creation of personal profiles could infringe the profilers' First Amendment rights. See Comments of Mead Data Central, Inc. and Dun & Bradstreet Corporation at 9-23; Comments of Information Industry Association at 8-10.

25 Comments of Time Warner Inc. at 17.

26 The proposed data base would have contained such personal information as the name, sex, age, estimated income, purchasing habits, and marital status of 120 million Americans. See Piller, *supra* note 5, at 11 (noting that Equifax received 30,000 angry letters from consumers protesting Marketplace plan); See also Daniel Mendel-Balck & Evelyn Richards, *Peering into Private Lives*, Wash. Post, Jan. 20, 1991, at H1.

sary.²⁷ Further, they cite examples of voluntarily adopted privacy codes that regulate the disclosure and use of personal information.²⁸

Of course, none of these examples suggests that market forces have prevented the creation and use of marketing profiles. Without question, public records, internal records, and external records are being accessed and matched into marketing profiles. Indeed, profilers have shown much ingenuity. For example, one way for a merchandiser to acquire more telling internal records is to issue a merchandiser credit card that is co-branded with a national credit card chain such as Mastercard or Visa. As provider of the credit card, the merchandiser has complete access to the credit card holder's transaction history, including the individual's shopping history at competing stores. By issuing such credit cards, merchandisers get "a tantalizing glimpse at what its shoppers buy from rivals."²⁹ This information is then used to market the card holder for the merchandiser's own products.

There is evidence, however, that market forces have prevented curious members of the public from accessing marketing profiles. Many list-compilers emphasize that their databases are used only for marketing, not to satisfy anyone's idle curiosity. For instance, it is the official policy of Donnelley Marketing Inc. and Database America Co., both national list-compilers, not to allow their national consumer database to be accessed for non-business purposes.³⁰

27 See Comments of GTE Services Corp. at 3 (existing business relationship between customers and service providers naturally provides privacy safeguards); Comments of AT&T at 8 (stating "Firms operating in competitive markets *must* honor reasonable customer expectations of privacy in the use of individually-identifiable information, or risk losing customers to competitors who are willing to respect and fulfill those expectations."); Comments of Southwestern Bell at 3 (stating that "If a company violates the expectations of its customers, over time that company is unlikely to continue [the] commercial relationship..."); Supp. Comments of Direct Marketing Association at 9 (noting that DMA fully appreciates that industry cannot thrive without consumer confidence and trust and "did not become a multi-billion dollar industry in the era preceding the NII by ignoring its customers.").

28 See generally *Privacy and American Business, Handbook of Company Privacy Codes* 20 (1994) (hereinafter *Privacy and American Business*) (compiling industry codes); Direct Marketing Association, *Fair Information Practices Manual: A Direct Marketer's Guide to Effective Self-Regulatory Action in the Use of Information* (1994).

29 Bird, *supra* note 6, at B12.

30 See Telephone Conversation with Harry Kitchen, Director of Database Analysis at Donnelley Marketing, Inc., September 29, 1994; Letter from Paul Sobel, Senior Vice President, Database America Companies, to Jerry Kang (Oct. 11, 1994) (explaining that its software is not configured to answer queries about specific individuals) (on file at NTIA).

In contrast, marketing profiles maintained by companies such as Lexis/Nexis—which contain personal information derived principally from public records—can be accessed by anyone who can afford the on-line charges. Another company, American Information Network, Inc., acts as an electronic information broker that can supply, among other information, criminal, driving, credit, motor vehicle, and property records. Also offered are license plate searches, national social security number locators, national address locators, workers' compensation records, and state corporate records. In addition, with increasing amounts of public record and other information available on-line, it has become easier to compile public record profiles by oneself. See

Also, comments received by NTIA did not reveal incidents of profilers obtaining external records at the transactional data level of detail. Profilers apparently obtain personal information from third parties in the form of mailing lists—complete or customized—which lack some of the details that transactional records tend to reveal.³¹ In particular, the comments described no instance in which profilers had official, authorized access to transactional records from payment providers, such as credit card companies. For example, American Express and Citibank have adopted policies that prohibit the disclosure of transactional records to third parties without customer consent, unless such disclosure is required by law.³² This is not, however, to say that electronic payment providers disclose absolutely no personal information to profilers. For example, both American Express and Citibank sell customized mailing lists of cardholders (names, addresses, and telephone numbers), generated by profiling cardholders in-house on the basis of their purchases.³³ Depending on how customized the list is, it may be nearly as sensitive as transactional data.

Besides transaction facilitators such as credit card companies, profilers can obtain external records from parties that transact directly with the individual to provide some product or service. These transacting parties include, for example, other merchandisers,

Pritchard-Schoch & Hutchens, *supra* note 3, at 14 (“Approximately 90% of the nation’s millions of public records are not yet accessible remotely Nonetheless, the market for online access to public records continues to experience steady growth, especially due to the demands of insurance companies, law firms, private investigators, and financial institutions.”).

- 31 For example, the industry advertisements and promotional materials of major list-compilers suggest that while they may know whether an individual holds a major credit card or not (by getting complete lists from credit card companies), they do not know what specific purchases have been made with that credit card. Similarly, although major list-compilers may know whether an individual subscribes to magazines (by getting complete lists from publishers), they do not seem to know which particular magazines one orders. Finally, although they may know whether an individual has made political contributions, they do not seem to know to whom, when, and how much.
- 32 See *Privacy and American Business*, *supra* note 28, at 20 (“We will release individual information about direct American Express customers only if the customer has consented . . . or when we are required to do so by law”); Citibank states that it “will not reveal specific information about a customer transaction (what, where, when, how much) to third parties except as previously disclosed to the customer in any communications and agreements.” *Id.* at 27.
- 33 In its “Privacy Notice to Cardholder” American Express states: “We [American Express] try to make sure that [promotional] offers reach only those card members most likely to take advantage of them. To do this, we develop lists for use by us and our affiliates based on information you provided on your initial application and in surveys, information derived from how you use the Card that may indicate purchasing preferences and lifestyle, as well as information available from external sources including consumer reports. We may also use that information, along with non-credit information from external sources, to develop lists which are used by the companies with whom we work.” *Privacy and American Business*, *supra* note 28, at 16.

Citibank’s notice contains a similar message: “If we [Citibank] find a product or special offer that we think would be of interest to you, we work with the companies involved to let you know by mail or phone.” See *id.* at 24; see also Jeff Smith, *Privacy Policies and Practices*, 36 Comm. of the ACM 104 (1993) (describing one credit card company in its survey used “cardholders’ purchases to create psychographic purchasing profiles”).

mail-order companies, and entertainment and information providers. The comments generated little information about the privacy policies of these varied transacting parties.³⁴ It is widely known that magazine publishers and book and music clubs often sell information about their customers to other merchandise profilers. However, NTIA received little comment on how exactly this information is divulged—as a complete mailing list (*e.g.*, entire clientele of a CD club), customized mailing list (*e.g.*, classical music buyer), or transactional data (*e.g.*, a particular individual purchased Vivaldi's Four Seasons in a particular month).

34 Commenters provided some information about an important source of TRPI—national on-line services. Two major on-line services—America Online and CompuServe—disclose personal information in the form of customized mailing lists created by profiling their subscribers on the basis of the transactions they make on-line. Compuserve sells mailing lists to third-parties “broadly based on member segments or selections,” *Communications Daily*, October 25, 1994, at 3 (electronic version), making available “interest categories which represent the on-line use of CompuServe members.” *Id.* (quoting Direct Media, list-compiler). Similarly, America Online sells personal information on its subscribers: name, addresses, [and] *type of customer*. *Communications Daily*, October 26, 1994, at 4 (electronic version) (emphasis added). Both America Online and Compuserve allow individuals to opt-out of such mailing lists.

In contrast, Prodigy has a policy of not disclosing any personal information about its subscribers to third-parties. Prodigy Services Co., *Policy on Protecting Member Privacy* (on file at NTIA). In addition, Apple Computer, Inc. (AppleLink, Eworld), Delphi Internet Services Corp., New York Times Service/Syndication, ProductView Interactive, and Dow Jones & Co., Inc., have internal policies prohibiting release of personal information to third parties. *See Communications Daily*, October 26, 1994 (electronic version).